Department of Homeland Security Daily Open Source Infrastructure Report for 11 August 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks

For info click here http://www.dhs.gov/

Daily Highlights

- The Washington Post reports a laptop computer from the inspector general's office at the Florida Department of Transportation was stolen last month, putting the sensitive personal information of nearly 133,000 Florida residents at risk. (See item 9)
- The Department of Homeland Security is taking immediate steps to increase security measures in the aviation sector in coordination with heightened security precautions in the United Kingdom, and has raised the threat level to High, or Orange, for all commercial aviation operating in or destined for the United States. (See item 12)
- The Associated Press reports investigators in southeast Ohio said they were working to unravel how two Michigan men charged with supporting terrorism came to have airplane passenger lists and airport security information. (See item 13)
- The BBC reports homes and businesses across England are being searched and 24 people questioned after police say a plot to blow up planes flying to the U.S. −− possibly in the next few days −− was disrupted; arrests in Pakistan were coordinated with arrests in the UK. (See item 17)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber:

ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 10, Reuters* — **Florida Gas again issues shipper alert due to heat.** Florida Gas Transmission on Thursday, August 10, issued an overage alert, the latest in a string of warnings to natural gas shippers in the past few months, as warm, humid weather boosts demand on its pipeline system. To maintain system integrity, the company issued an overage alert at 25 percent tolerance, meaning shippers must stay within 25 percent of scheduled volumes, the company said in a Website posting. Alerts, also called critical days, require natural gas shippers to adhere carefully to scheduled quantities. An overage alert signals that taking excess quantities off line would be harmful. Florida Gas regularly issues alerts as temperatures in the state vary extremely from normal, boosting gas and power demand as needed. The 5,000−mile Florida Gas Transmission pipeline runs from southern Texas to southern Florida, with a mainline capacity of 2.1 billion cubic feet per day.
Source: http://yahoo.reuters.com/news/articlehybrid.aspx?storyID=urn:newsml:reuters.com:20060810:MTFH68560_2006−08−10_17−08−29_N10468022&type=comktNews&rpc=44

2. *August 10, Associated Press* — **PG & E plans solar energy purchase.** PG & E Corp.'s Pacific Gas and Electric utility said Thursday, August 10, it signed a contract with Luz II LLC to buy solar energy beginning in the spring of 2010. Luz plans to build hybrid solar−gas design plants that can dispatch electricity all day, pending regulatory approval. Pacific Gas agreed to buy at least 500 megawatts of solar energy from Luz that will power up to 350,000 customers. PG & E currently plans to add 300 megawatts of renewable electric power a year to its supply. This includes wind, solar, geothermal and other forms of renewable energy.
Source: http://www.chron.com/disp/story.mpl/ap/fn/4108483.html

3. *August 09, Associated Press* — **El Paso Corp. to raise rates on Colorado system.** Natural gas distributor El Paso Corp. on Wednesday, August 9, said its Colorado Interstate Gas Co. unit has received federal regulatory clearance to raise rates on its pipeline transmission system. The Federal Energy Regulatory Commission approved Colorado Interstate's rate case, which preserves the current state of services but allows for rate increases. Rates have not been changed for the last five years, El Paso said. Colorado Interstate Gas serves Public Service Co. of Colorado, which supplies utilities and other customers in the state with natural gas.
Source: http://biz.yahoo.com/ap/060809/el_paso_rate_change.html?.v=2

4. *August 09, Reuters* — **Alaska launches BP probe.** Alaska Governor Frank Murkowski suggested on Wednesday, August 9, that BP Plc misled the state with satisfactory maintenance reports and launched an investigation into the oil giant's handling of its pipeline corrosion. Pipeline corrosion forced BP to halt production at its Prudhoe Bay field and the company is studying whether it needs to shut down the entire 400,000 barrels−per−day field, which accounts for eight percent of U.S. output. The governor said Alaska's attorney general is looking into possible enforcement actions, including a demand for lost tax revenues while the field is shut down. After "numerous" satisfactory maintenance reports to the state in the past that oil−field pipeline corrosion was being adequately controlled, BP abruptly decided to shut down Prudhoe Bay without consulting the state, Murkowski said. "We will hold British Petroleum accountable for past and future field management decisions," Murkowski told a joint

session of the legislature in Juneau. Alaska House Speaker John Harris said lawmakers plan a series of hearings into pipeline corrosion starting next week.
Source: http://news.moneycentral.msn.com/provider/providerarticle.asp?feed=OBR&Date=20060809&ID=5937013

[Return to top]

Chemical Industry and Hazardous Materials Sector

5. *August 10, WHIO−TV 7 (OH)* — **Leaking diesel fuel causes highway shutdown in Ohio.** A truck in Dayton, OH, caused problems Thursday morning, August 10, for motorists on Interstate 75 when a piece of sheet metal pierced the truck's fuel tank, causing about 100 gallons of fuel to start leaking. Police said two lanes of the highway were closed down to clean up the spill.
Source: http://www.whiotv.com/news/9659945/detail.html?rss=day&psp=n ews

[Return to top]

Defense Industrial Base Sector

6. *August 09, Aviation Now* — **Pentagon finalizes changes in JTRS management.** Under a new management plan finalized by the Pentagon, the military's proposed Joint Tactical Radio System (JTRS) will have centralized funding, engineering and program development authority. Approved by Defense Deputy Secretary Ken Krieg, the plan consolidates authority, direction and control of JTRS by the joint program executive officer through the Navy. The Pentagon released details of the new arrangement on Tuesday, August 8. Under the changes, the roles and responsibilities are better defined for JTRS' acquisition management as well as technical, fiscal, managerial and personnel control. The changes also should streamline internal program reporting and ensure the advisory roles for the agencies and businesses involved in the program for resources, requirements and acquisition.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/JTRS08096.xml

[Return to top]

Banking and Finance Sector

7. *August 10, Silicon* — **Security experts downplay HSBC's online banking flaw.** Security professionals have questioned reports of a "serious flaw" in HSBC's online banking system. Researchers at Cardiff University claim to have discovered the flaw which, according to The Guardian, over two years left 3.1 million customers exposed due to a defect in how people access their online accounts. The vulnerability, which was not detailed in the researchers' report, relies on a hacker using a keystroke logger. Graham Cluley, senior technology consultant for antivirus company Sophos, said: "Unless Cardiff gives some more information, it's a non−story −− there's no meat on this." To access HSBC's banking Website, users are required to enter an alpha−numeric password, a date of birth then a PIN. Cardiff University

claims that any account can be broken into within nine attempts of hacking the Website, though first the hackers would need to plant a keystroke logger on the victim's PC. Cluley added: "They could gather [PIN] digits in up to nine attempts but it doesn't seem a very effective way of doing this."
Source: http://www.silicon.com/financialservices/0,3800010364,391613 20,00.htm

8. *August 10, Honolulu Advertiser* — **Hawaiian Tel Federal Credit Union warns of scam.** Hawaiian Tel Federal Credit Union has joined Bank of Hawaii, First Hawaiian Bank and American Savings Bank as a target of Internet−based thieves trying to scam money out of customers through phony e−mails. The credit union said thieves sent e−mails to some Hawaii residents last week trying to get them to give information about ATM or debit cards. Hawaiian Tel Federal Credit Union said it alerted members about the bogus mailing, notified the National Credit Union Administration about the attack and worked with vendors to get a Website related to the scam taken down.
Source: http://www.honoluluadvertiser.com/apps/pbcs.dll/article?AID= /20060810/BUSINESS1301/608100316/1071

9. *August 10, Washington Post* — **Laptop stolen from Florida Department of Transportation −− nearly 133,000 affected.** A laptop computer from the inspector general's office at the Department of Transportation was stolen last month, putting the sensitive personal information of nearly 133,000 Florida residents at risk, acting Inspector General Todd J. Zinser said Wednesday, August 9. The laptop, assigned to a special agent in the Miami office, was stolen from a government vehicle on July 27 in Doral, FL, Zinser told Florida Governor Jeb Bush Wednesday in a letter. The computer, which requires a password to operate, contains the unencrypted names, Social Security numbers, birth dates and addresses of 42,792 Florida residents who hold a pilot's license; 80,667 people in the Miami−Dade County area who hold a commercial driver's license; and 9,496 people who were issued a personal or commercial driver's license in the Tampa area, the letter said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08 /09/AR2006080901177.html

10. *August 09, Websense Security Labs* — **Phishing Alert: First National Bank of Greencastle.** Websense Security Labs has received reports of a new phishing attack that targets customers of First National Bank of Greencastle. Users receive a spoofed e−mail, which says that they have been chosen to earn $100 if they complete an online survey. The spoofed e−mail instructs users to click on a link that redirects them to a fraudulent site. Users who visit this Website are prompted to enter their account password and credit card information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=572

11. *August 08, Websense Security Labs* — **Phishing Alert: Penn State Federal Credit Union.** Websense Security Labs has received reports of a new phishing attack that targets customers of Penn State Federal Credit Union. Users receive a spoofed e−mail that claims new security standards have been implemented and account details need to be confirmed. The spoofed e−mail instructs the user to click on a link that redirects them to a fraudulent site. Users who visit this Website are prompted to enter their account password and credit card information.
Source: http://www.websense.com/securitylabs/alerts/alert.php?AlertI D=571

[Return to top]

Transportation and Border Security Sector

12. *August 10, Department of Homeland Security* — **Statement announcing a change to the nation's threat level for the aviation sector.** The Department of Homeland Security is taking immediate steps to increase security measures in the aviation sector in coordination with heightened security precautions in the United Kingdom. Over the last few hours, British authorities have arrested a significant number of extremists engaged in a substantial plot to destroy multiple passenger aircraft flying from the United Kingdom to the United States. Currently, there is no indication, however, of plotting within the United States. We believe that these arrests have significantly disrupted the threat, but we cannot be sure that the threat has been entirely eliminated or the plot completely thwarted. For that reason, the United States Government has raised the nation's threat level to Severe, or Red, for commercial flights originating in the United Kingdom bound for the United States. To defend further against any remaining threat from this plot, we will also raise the threat level to High, or Orange, for all commercial aviation operating in or destined for the United States. Consistent with these higher threat levels, the Transportation Security Administration is coordinating with federal partners, airport authorities, and commercial airlines on expanding the intensity of existing security requirements. Travelers should also anticipate additional security measures within the airport and at screening checkpoints.
Official remarks on aircraft threats:
http://www.tsa.gov/press/releases/2006/press_release_0810200 6b.shtm
Transportation Security Administration's new security measures:
http://www.tsa.gov/press/where_we_stand/security_measures.sh tm
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0974.xml

13. *August 10, Associated Press* — **Pair with passenger info, phones linked to terror.** Investigators in southeast Ohio said they were working to unravel how two Michigan men charged with supporting terrorism came to have airplane passenger lists and airport security information. Osama Sabhi Abulhassan, 20, and Ali Houssaiky, 20, both of the Detroit suburb of Dearborn, were being held at Ohio's Washington County jail on $200,000 bond each, which could be raised at a Thursday, August 10, court hearing. Each was charged Wednesday, August 9, with money laundering in support of terrorism. Deputies stopped the two on a traffic violation Tuesday and found the flight documents along with $11,000 cash and 12 phones in their car, Sheriff Larry Mincks said. It wasn't clear what significance the airline information might have. Assistant County Prosecutor Susan Vessels declined to comment on whether the manifests were for upcoming flights or those that already had flown. The fourth−degree felony charges allege the two laundered between $5,000 and $25,000, Vessels said. A conviction carries a maximum sentence of 18 months in prison and a $5,000 fine.
Source: http://www.usatoday.com/travel/news/2006−08−10−ohio−terror−s uspsects_x.htm

14. *August 10, Associated Press* — **Metro increases security as a precaution.** Washington, DC's Metro transit increased security on Thursday, August 10, as a precaution after a terror plot was disrupted in Britain, but officials say there is no threat to the transit system. Metro spokesperson Candace Smith says transit police will be doing random sweeps of stations throughout the day.

They are also closing all public bathrooms in Metro stations. Additional measures include increased security announcements and dumping trash cans more often.
Source: http://www.wusatv9.com/news/news_article.aspx?storyid=51339

15. *August 10, Washington Post* — **Security restrictions, delays at U.S. airports.** At airports in the Washington, DC, area and across the country, huge lines formed early Thursday morning, August 10, and flights were delayed for hours as officials implemented hastily devised new restrictions designed to ward off terror attacks. Shortly after British authorities announced the arrests of 21 people who allegedly were plotting to blow up jets flying from the United Kingdom to the United States, security officials tightened searches of carry−on luggage and banned cosmetic lotions, beverages, and other non−essential liquids from being brought on board. At Washington Dulles International Airport in Northern Virginia, frazzled airport employees handed time−stamped cards to passengers idling in long security lines, in an effort to gauge how long the wait would be. At Reagan Washington National Airport, passengers watched helplessly as their scheduled departure times slipped by. At Baltimore−Washington International Thurgood Marshall Airport, where the snaking lines filled the D concourse completely, police patrolled the perimeter of the surging crowd, carrying plastic handcuffs and automatic weapons. At airports across the United States, employees from the Transportation Security Administration distributed fliers outlining the new restrictions, and hauled out bins so passengers could dump toiletries, coffee, bottled water, and other banned items.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/10/AR2006081000416.html

16. *August 10, Financial Times (UK)* — **Restrictions cause chaos at UK airports.** Airports across the UK were thrown into chaos after the government imposed immediate hand luggage restrictions and extra security checks in the wake of Thursday, August 10's major anti−terrorist operation. The ban on all but essential hand luggage caused long delays at London Heathrow and other leading UK airports, prompting hundreds of flight cancellations by European airlines. British Airways said it had cancelled all short−haul flights to and from Heathrow Airport for the whole of the day. It added that some flights to and from Gatwick would be cancelled and that long−haul flights would be subject to delay. The Department for Transport advised passengers to stay at home unless their journeys were essential. Lufthansa, Iberia, and Olympic cancelled flights to the UK, and there were no flights from Brussels to London. Air France grounded all flights from Paris to Heathrow until congestion problems eased. There was a high police presence at major airports, as long queues grew to get into the busiest terminals, particularly Heathrow, Gatwick, Manchester and Stansted. The British hand luggage restrictions meant passengers could carry nothing in their pockets and were allowed only a plastic carrier bag.
Source: http://www.ft.com/cms/s/c7867418−2857−11db−a2c1−0000779e2340 .html

17. *August 10, BBC* — **UK police probe terror plot.** Homes and businesses across England are being searched and 24 people questioned after police say a plot to blow up planes from the UK to the U.S. was disrupted. They say they are convinced they have the key players in custody, but a wider investigation is only just beginning. Peter Clarke, the head of Scotland Yard's anti−terrorist branch, said the network involved was large and global. Sources in the UK have confirmed that they believe an attack may have been imminent −− possibly in the next few days. According to U.S. intelligence officials, the plotters hoped to stage a practice run within

two days, with the actual attack following within days. Security chiefs said the group had been under surveillance for some time, and believe they planned to detonate liquid explosives on up to 10 planes. The terrorists would have smuggled it on board hidden in drinks, electronic devices, and other "common objects." According to U.S. officials, the airlines targeted were United, American, and Continental. Foreign Office spokesperson Tasnim Aslam said, "Pakistan played a very important role in uncovering and breaking this international terrorist network. There were some arrests in Pakistan which were coordinated with arrests in the UK."
Source: http://news.bbc.co.uk/2/hi/uk_news/4780815.stm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

18. *August 10, Thanhniem News (Vietnam)* — **Foot−and−mouth disease in Vietnam capital.** Cattle and pigs in Hanoi's Thanh Tri district have manifested symptoms of foot and mouth disease, reported the local department of economic planning and rural development Wednesday, August 9. Two pigs have been destroyed to date, and cows have been found to have stopped eating due to the illness. The local department of economic planning and rural development in cooperation with the Health Animal Department has established two animal check points and isolated the infected cattle.
Source: http://www.thanhniennews.com/healthy/?catid=8&newsid=18697

19. *August 08, Canadian Food Inspection Agency* — **Bovine spongiform encephalopathy investigation in Manitoba completed.** The Canadian Food Inspection Agency (CFIA) has concluded its epidemiological investigation of the case of bovine spongiform encephalopathy (BSE) confirmed on July 3, 2006 in a cow from Manitoba. The advanced age of the affected animal −− at least 16 years old −− limited the CFIA's capacity to collect information concerning the animal's early history, including its birth farm. Investigators traced 21 herdmates that had been previously purchased with the affected animal. One of these animals was still alive and tested negative for BSE. Cattle are most susceptible to BSE infection during their first year of life. Therefore, this animal was likely exposed to the BSE agent in 1989 or 1990, at which time the use of meat and bone meal in cattle feed was an accepted and legal practice. Feed fed to this animal after the 1997 introduction of Canada's feed ban was found to be in compliance with regulatory requirements.
Source: http://www.inspection.gc.ca/english/corpaffr/newcom/2006/200 60808e.shtml

[Return to top]

Food Sector

20.

August 10, USAgNet — **Rules on bovine imports from Canada eased.** The U.S. Department of Agriculture (USDA) proposed on Wednesday, August 9, to allow imports of Canadian poultry and pork processed at plants that also handle cattle, in a sign of declining fears of mad cow disease. USDA now requires that Canadian meat products derived from non−ruminant poultry and pigs come from facilities separate from those processing ruminant animals such as cattle, which are susceptible to mad cow disease. Ruminant animals collect swallowed food in a part of their stomachs for further chewing. The USDA said because products derived from nonruminant animals pose a small risk of getting mad cow disease from contaminated products, it was "inconsistent" to have them processed in a separate facility.
Source: http://www.usagnet.com/story−national.php?Id=1578&yr=2006

21. *August 08, Cattle Network* — **Feed recall due to mammalian protein.** The U.S. Food and Drug Administration announced two recalls, one for 27 million pounds of feed produced in Michigan and the other an unknown amount of feed produced in Kentucky. Both were suspected of being adulterated with ruminant or mammalian protein, including ruminant meat and bone meal in the second recall. Vita Plus Corp., Gagetown, MI, has recalled 27,694,240 pounds of dairy feed produced between February of 2005 and June 16, 2006, because it is believed it was contaminated with mammalian protein. The feed was distributed in Michigan. Burkmann Feeds LLC, Glasgow, KY, has recalled an unknown amount of custom feed because it contains an ingredient called Pro−Lak, which may contain ruminant−derived meat and bone meal. The Burkmann feed was distributed in Kentucky.
Source: http://www.cattlenetwork.com/content.asp?contentid=58260

[Return to top]

Water Sector

22. *August 10, New York Times* — **As water grows scarce, corporations see profit.** A fresh group of big businesses is discovering there may be great profits in water. A United Nations study foresees five billion of the world's 7.9 billion people in 2025 facing a scarcity of clean water. Most analysts expect the water market in the U.S. to be worth at least $150 billion by 2010. And it may happen even sooner than that. Arid cities like Los Angeles and Phoenix already grapple with sporadic water shortages. New York City's water −− once lauded for its purity −− is getting cloudy, and the American Society of Civil Engineers has given the pipes and other parts of the country's water system a D minus. Globally, water problems are even more immediate. Many experts estimate that water−related equipment and services already make up a $400 billion global market. For now the water industry remains fragmented, with no company commanding more than five percent of sales. But it is consolidating rapidly. In 1999, there were 60 companies in the Palisades Water Index, a list of water company stocks. Today, the list is pared to 38.
Source: http://www.nytimes.com/2006/08/10/business/worldbusiness/10water.html?_r=1&oref=slogin

[Return to top]

Public Health Sector

23. *August 10, Associated Press* — **Bird flu monitoring expands nationally.** Monitoring of wild migratory birds to prevent a deadly bird flu virus is expanding to cover the entire nation and U.S. territories in the Pacific. The stepped−up testing will be done by scientists in the lower 48 states, Hawaii and other Pacific islands. They will begin keeping an eye out for the H5N1 strain of the avian flu that has killed more than 100 people, mostly in Asia. In Alaska, where the first migratory birds began arriving, monitoring started just before summer. Feces or tissue samples from 75,000 to 100,000 wild birds will be collected, along with 50,000 samples of the water and ground that birds come into contact with. Locations where the samples will be collected will vary depending on weather and habitat conditions. Likely sites include national and state wildlife refuges and parks, city ponds and parks, and private lands where owners have given approval.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/08/10/AR2006081000232.html

24. *August 07, Lawrence Livermore National Laboratory* — **Nanowire 'barcode' system speeds biodetection in the field.** Detecting biowarfare agents in the field will become a lot easier thanks to a new barcode system based on biosensing nanowires developed by Lawrence Livermore National Laboratory (LLNL) researchers. Multi−striped nanowires allow rapid and sensitive immunoassays for biowarfare agent simulants. The researchers built submicrometer layers of different metals including gold, silver and nickel that act as "barcodes" for detecting a variety of pathogens ranging from anthrax, smallpox and ricin to botulinum. The team, led by LLNL and including researchers from Stanford University, the University of California−Davis Center for Biophotonics and Nanoplex Technologies, used the multi−striped metallic nanowires in a suspended format to rapidly identify sensitive single and multiplex immunoassays that simulated biowarfare agents. The researchers produced nanoscale wires by electrochemically depositing metals within the tiny cavities of porous mineral solids. They then layered the gold and silver in a specific way to produce nanowires with different characteristic stripe patterns depending on which pathogen they were trying to identify. The reflection pattern and fluorescence from each stripe sequence can later be clearly recognized, similar to a barcode on a retail product. The system not only applies to biowarfare agents, but could also be used during an outbreak of an infectious disease.
Source: http://www.llnl.gov/pao/news/news_releases/2006/NR−06−08−01. html

25. *August 07, USA Today* — **Diagnoses at the click of a mouse.** Rapid diagnosis could help save a patient's life and prevent the disease from spreading through the hospital and out into the community. But most American medical workers have never seen a case of bird flu. The deadly H5N1 strain that emerged in Hong Kong in 1997 and has spread in Asia and Europe since 2003 has not been found in the U.S., but health officials are urging doctors to be on alert for it. Now, a new tool being used in hundreds of hospitals and clinics could help doctors and nurses quickly differentiate between infection with the H5N1 virus and 40 other respiratory diseases. The Acute Pulmonary Infections program is the latest addition to a computer software system used in 350 hospitals in the U.S. and 10 other countries, along with the U.S. military and several state and local health departments. The system provides instant access to nearly 13,000 medical photos that can help doctors diagnose more than 700 diseases, drug reactions or infections.
Source: http://www.usatoday.com/tech/news/techinnovations/2006−08−07

−visualdx−bird−flu_x.htm?POE=TECISVA

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *August 10, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical Activity: Atlantic/Gulf of Mexico/Caribbean Sea: A strong, well−defined tropical wave is set to enter the eastern Caribbean Sea. It is along 59W south of 20N and moving west 23 mph. The system currently is poorly organized −− it still has the potential to develop into a tropical depression during the next 24 to 36 hours. An Air Force reserve hurricane hunter aircraft is scheduled to investigate the system on Thursday, August 10 if necessary.
Earthquake Activity: A magnitude of 4.1 (light) earthquake occurred Thursday, August 10 at 4:52 a.m. EDT. The quake was centered 84 miles east−southeast of Anchorage, Alaska at a depth of 9.3 miles. There have been no reports of damages or injuries.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat081006.shtm

27. *August 10, St. Louis Post−Dispatch* — **Massive emergency drill held at Busch Stadium in St. Louis, Missouri.** The massive emergency response drill at Busch Stadium in St. Louis, MO on Wednesday, August 9 started not with a bang but with a downpour. The dozens of agencies involved had planned a number of fake disasters −− including a chlorine tanker rupturing on I−64, weapons of mass destruction smuggled into the ballpark in backpacks, and a possible threat to first responders. Nature played along with the thousands of people who volunteered to play victims and bystanders by providing a fierce thunderstorm as everyone was arriving at Busch for the drill in the early evening, triggering an almost two−hour rain delay. "We won't know how everything went for some time, but I think it's already a success," St. Louis Police Chief Joe Mokwa said. "Working under a unified command, having everyone dress out, the experience and joint effort −− it's invaluable." Another mock emergency will take place Thursday, August 10 at a roller rink in Olivette, MO.
Source: http://www.stltoday.com/stltoday/news/stories.nsf/metroeast/story/80A252834034BDF1862571C60011B92F?OpenDocument

28. *August 09, AzJournal (AZ)* — **Disaster drill will test responders in Arizona on September 22.** On Friday, September 22, a Department of Homeland Security full−scale exercise will be conducted at the Navajo County fairgrounds in Holbrook, AZ. More than 300 first responders will participate, including personnel from Navajo, Apache and Coconino counties, cities within those counties, and state and private agencies from as far away as Tucson. Navajo County Emergency Services Director Larry Dunagan explained that several mock emergency situations will be created, and the responders will have to handle them as if they were actual emergencies.

The exercises will require close cooperation among the responders. The purpose is to establish communication between various agencies and government officials, and to test emergency plans for flaws.
Source: http://www.azjournal.com/pages/news/2006/August06/080906EmergencyExercise.html

[Return to top]

Information Technology and Telecommunications Sector

29. *August 10, VNUNet* — **Kaspersky: Evolved worms target all IM networks.** According to Kaspersky, there will be a sharp rise in next−generation IM worms which can spread via multiple IM networks, triggering the demise of traditional IM worms, such as Bropia, Kelvia and Prex, which spread via single IM networks, such as MSN. IM worms, such as IRCBot.lo, will represent the greatest IM threat, as they can spread to a large number of networks and can use variable messages and download links, the security firm warned.
Source: http://www.vnunet.com/vnunet/news/2162071/evolved−worms−targ et−im

30. *August 09, Security Focus* — **Cisco Internet Key Exchange denial−of−service vulnerability.** Cisco Internet Key Exchange (IKE) is prone to a denial−of−service vulnerability. This issue affects devices implementing IKE version 1 and is due to a resource exhaustion when handling a high rate of IKE requests. An attacker can exploit this issue through continuous attacks to deplete the available resources. This will cause the device to deny future connections and to block current connections that are re−keyed.
For a complete list of vulnerable products: http://www.securityfocus.com/bid/19176/info
Solution: Currently, Security Focus is not aware of any vendor−supplied patches for this issue.
Source: http://www.securityfocus.com/bid/19176/references

31. *August 09, Tech Web* — **Exploit for worst bug of August on the loose.** A day after Microsoft posted a dozen patches for Windows and Office, the one pegged by security analysts as the most dangerous is being used in attacks, the federal cyber−agency said. According to an advisory issued Wednesday, August 9, by the U.S. Computer Emergency Readiness Team, or US−CERT, the arm of the Department of Homeland Security that disseminates information about developing computer threats, an active exploit of the buffer overflow bug in Windows' Server service has been confirmed. "If a remote attacker sends a specially crafted packet to a vulnerable Windows system, that attacker may be able to execute arbitrary code with system privileges," US−CERT said in the warning. In its MS06−040 security bulletin, Microsoft spelled out the problem with Server service, a component responsible for sharing of local resources such as drives and printers, with others on the network. Attackers could exploit the buffer overflow vulnerability, Microsoft said, without any user intervention. "While we always recommend applying any updates rated "Critical" as soon as possible, we are recommending that customers give priority to MS06−040 for testing and deployment due to technical specifics around the vulnerability," the Microsoft Security Response Center advised.
US−CERT Advisory: http://www.us−cert.gov/current/current_activity.html#msvuls
MS06−040 Security Bulletin: http://www.microsoft.com/technet/security/Bulletin/MS06−040.mspx
Source: http://www.techweb.com/wire/security/191900653;jsessionid=Q5

TOTRIZDC5AMQSNDLPSKHSCJUNN2JVN

32. *August 09, CRN* — **Researcher: Hacker sophistication outpacing forensics.** Speaking at the Black Hat conference in Las Vegas last week, Kevin Mandia, president of Mandiant, an Alexandria, VA−based security consultancy, said attackers are using increasingly sophisticated methods to evade detection and make life difficult for security incident response teams. The sophistication of hackers' tools is outpacing that of investigators' forensic tools, and one of the consequences is that incident response teams charged with investigating attacks on networks are taking between five and eight days to find malicious code, Mandia said. Although Windows security breaches make up the majority of security incidents, the kernel level rootkits Mandia has come across thus far have been Linux−based. Mandia said the main reason hackers aren't running kernel level rootkits is because they can make systems unstable, which could blow their cover. Other common indicators that a PC's security has been breached include the inability to execute a 'save as' command; continual termination of antivirus software; and Windows Task Manager closing immediately when a user executes a 'ctrl−alt−delete' command, according to Mandia.
Source: http://www.crn.com/showArticle.jhtml?articleID=191900748

33. *August 09, Tech Web* — **Abuse of insider security privileges often goes unmonitored.** As the keepers of the keys, IT and security staff have the best chance to access sensitive corporate data without being detected. Of course, some functions require security staffers to access, even read, sensitive documents as part of everyday system surveillance, an audit, or an investigation of suspected policy violations. However, when an IT staffer is unhappy or disgruntled, the abuse of security privileges can escalate to a much more threatening level. In fact, 86 percent of "insider" computer sabotage −− malicious system attacks that don't involve fraud or information theft −− is perpetrated by employees in technical positions, according to a study published last year by the U.S. Secret Service's National Threat Assessment Center and the Carnegie Mellon Software Engineering Institute's CERT Program. It's difficult to quantify the online behavior of IT people, principally because they are capable of excluding themselves from most efforts to analyze online activity. In most cases, though, the abuse of security privileges leads to more snooping than sabotage. Even in those cases, however, it's a good idea to have the ability to monitor IT staffers' behavior.
Source: http://www.darkreading.com/document.asp?doc_id=100932

Internet Alert Dashboard

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 4672 (eMule), 445 (microsoft−ds), 65530 (WindowsMite), 54856 (−−−), 80 (www), 32790 (−−−), 113 (auth), 39972 (−−−), 135 (epmap) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

34. *August 10, Associated Press* — **Statue of Liberty's crown to stay closed.** Tourists won't be climbing back up to the Statue of Liberty's crown. That's the word from the National Park Service to lawmakers, some of whom have been fighting to reopen the crown following the 2001 terror attacks. The crown has been closed out of concerns that fire and terrorism hazards for the cramped spiral staircase could not be overcome. A congressman, who oversees the House subcommittee on national parks, said he may hold hearings to re−examine the issue and the agency's decision. "While I respect the Park Service's justified concern for public safety, I am disappointed...." said Rep. Steve Pearce, (R−NM). Outgoing Park Service Director Fran Mainella said that even before 2001, the park service had been re−evaluating public safety at the statue, particularly concerns about fire safety on the 168−step ascent from the base to the crown. She said the crown was originally designed for maintenance workers, not the public.
Source: http://www.usatoday.com/news/nation/2006−08−09−statue−libert y−crown_x.htm

35. *August 10, Associated Press* — **Extra police at the Indiana State Fair.** Police boosted security in and around the Indianapolis state fairgrounds to help ensure that the Indiana State Fair isn't marred by the sort of violence that's left 13 people in the city dead in recent days. Thousands of out−of−town visitors began converging on the 250−acre fairgrounds Wednesday, August 9, for the 150th fair. The site is surrounded by troubled lower−income neighborhoods, including one six blocks away where a teenage boy was shot to death Monday. The extra security is part of the city's response to 13 slayings since August 2, which includes stepped−up police patrols in the city's trouble spots and lengthening officers' shifts by two hours, said Indianapolis Police Department spokesman Maj. Lloyd Crowe. About 300 officers or security guards will be posted at the fair during its 12−day run, including about 130 state troopers, 40 state conservation officers and some 50 private security guards, said fair spokesperson Andy Klotz. The fair, which averages about 40,000 to 120,000 visitors a day depending on the day and weather, has been incident−free over the years.
Source: http://abcnews.go.com/US/LegalCenter/wireStory?id=2295860

[Return to top]

General Sector

36. *August 10, Associated Press* — **Six of 11 missing Egyptian students now in custody; more arrests made.** Six of the 11 Egyptian exchange students who failed to show up for their college program are now in custody after three additional students were arrested Thursday, August 10, the FBI said. El Sayed Ahmed Elsayed Ibrahim, 20, and Alaa Abd El Fattah Ali El Bahnasawi, 20, were arrested at a residence in Dundalk, MD, by U.S. Immigration and Customs Enforcement agents. Chicago police detained Ahmed Mohamed Mohamed Abou El Ela, 22, at OHare International Airport as he was attempting to book a flight to Montana, the FBI said. All are being held on immigration violations because they did not report on time to their month−long program at Montana State University in Bozeman, MT. The other five Egyptians still are being sought.
Source: http://www.usatoday.com/news/nation/2006−08−10−missing−egypt

ian−students_x.htm

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer